Homework 2

Mark Schulist

1)

×	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Table 1: Multiplication table for $\mathbb{Z}/6\mathbb{Z}$

2)

2.a)

$$\begin{aligned} f : \mathbb{Z}/11\mathbb{Z} &\to \mathbb{Z}/11\mathbb{Z} \\ x &\mapsto x^3 - 2x^2 + 4 \end{aligned} \tag{1}$$

$$f(5) = 79 \equiv 2 \bmod 11 \tag{2}$$

2.b)

- 0 is not invertible because $0x = 0$ for any $x \in \mathbb{Z}/11\mathbb{Z}$
- 1 is invertible because $1 \cdot 1 \equiv 1 \bmod 11$
- $2 \cdot 6 \equiv 1 \bmod 11$
- $3 \cdot 4 \equiv 1 \bmod 11$
- $4 \cdot 3 \equiv 1 \bmod 11$
- $5 \cdot 9 \equiv 1 \bmod 11$
- $6 \cdot 2 \equiv 1 \bmod 11$
- $7 \cdot 8 \equiv 1 \bmod 11$
- $8 \cdot 7 \equiv 1 \bmod 11$
- $9 \cdot 5 \equiv 1 \bmod 11$
- $10 \cdot 10 \equiv 1 \bmod 11$

2.c)

$$5x \equiv 3 \bmod 11 \tag{3}$$

$$\begin{aligned} 9(5x) &\equiv 3 \cdot 9 \bmod 11 \\ \implies \quad x &\equiv 27 \bmod 11 \\ \implies \quad x &\equiv 5 \bmod 11 \end{aligned} \tag{4}$$

3)

3.a)

Proof.

$$\begin{aligned} n-1 &\equiv -1 \bmod n \\ (n-1)^{100} &\equiv 1 \bmod n \end{aligned} \tag{5}$$

Therefore, $(n-1)^{100}$ is congruent to $1 \bmod n$. Because $(n-1)^{100}$ is congruent to $1 \bmod n$, it is always 1 larger than a multiple of n by definition of modulo. □

3.b)

Proof.

$$(n-2)^6 \equiv 33 \bmod n \tag{6}$$

Therefore, n must divide $33 - (n-2)^6$.

$$\begin{aligned} n &\mid 33 - (n-2)^6 \\ n &\mid 33 - \underbrace{n(...)}_{n \text{ divides}} - 2^6 \\ n &\mid 33 - 2^6 \\ n &\mid -31 \end{aligned} \tag{7}$$

So n must divide -31. Because 31 is prime, the only possible positive values for n are 31 or 1. □

3.c)

Proof.

$$7^n \equiv 17^n \bmod 8 \tag{8}$$

We know that $7 \equiv -1 \bmod 8$ and $17 \equiv 1 \bmod 8$, so we can insert these facts into the given equation.

$$\begin{aligned} 1^n - (-1)^n &\equiv 0 \bmod 8 \\ 1^n &\equiv (-1)^n \bmod 8 \end{aligned} \tag{9}$$

This is only true when n is even, so n must be even. □

3.d)

Proof.

$$3^n \equiv r \bmod 13 \tag{10}$$

There are 3 cases (when n is 0, 1, or 2 greater than a multiple of 3).

If $n = 3k$ for some $k \in \mathbb{Z}$:

$$\begin{aligned} 3^{3k} &\equiv r \bmod 13 \\ 27^k &\equiv r \bmod 13 \\ 1^k &\equiv r \bmod 13 \end{aligned} \tag{11}$$

Therefore, if n is a multiple of 3, then r will be 1.

If $n = 3k + 1$ for some $k \in \mathbb{Z}$:

$$\begin{aligned} 3^{3k+1} &\equiv r \bmod 13 \\ 3 \cdot 3^{3k} &\equiv r \bmod 13 \\ 3 \cdot 1 &\equiv 1 \bmod 13 \end{aligned} \tag{12}$$

So if n is one more than a multiple of 3, then r will be 3.

If $n = 3k + 2$ for some $k \in \mathbb{Z}$:

$$\begin{aligned} 3^{3k+2} &\equiv r \bmod 13 \\ 9 \cdot 1 &\equiv r \bmod 13 \end{aligned} \tag{13}$$

So if n is two more than a multiple of 3, then r will be 9. □

4)

4.a)

$$a \in \mathbb{Z}, b = 2k + 1 \tag{14}$$

Proof.

$$\begin{aligned} a^2 + 2b &= a^2 + 2(2k + 1) \\ &= a^2 + 4k + 2 \end{aligned} \tag{15}$$

AFSOC that there exists a number (x) that when squared, equals $a^2 + 4k + 2$.

We can use the fact that $x^2 \equiv 0, 1 \bmod 4$ (x^2 cannot be congruent to 2 or 3 mod 4).

$$\begin{aligned} x^2 &\equiv a^2 + 4k + 2 \bmod 4 \\ 2 &\equiv a^2 - x^2 \bmod 4 \end{aligned} \tag{16}$$

There are no values for x and a where this equation is true. The only possible values it can be are 0, 1, or 3. Hence, $a^2 + 2b$ cannot be a perfect square. □

4.b)

Proof.

$$n \equiv 4 \bmod 5 \tag{17}$$

$$\begin{aligned} 0^4 &\equiv 0 \bmod 5 \\ 1^4 &\equiv 1 \bmod 5 \\ 2^4 &\equiv 1 \bmod 5 \\ 3^4 &\equiv 1 \bmod 5 \\ 4^4 &\equiv 1 \bmod 5 \end{aligned} \tag{18}$$

The maximum value for a^4 (and b^4 and c^4) in mod 5 is 1 (and the only other value is 0), so $1 + 1 + 1$ is the largest value $a^4 + b^4 + c^4$ can take, which is less than n, which itself is congruent to 4 mod 5.

In other words, $a^4 + b^4 + c^4 \equiv 3 \bmod 5$ is the largest value this sum can take on, so it can never be congruent to 4 mod 5. □

5)

$$11 \mid n \Longleftrightarrow 11 \mid a_0 - a_1 + a_2 - a_3 + \ldots + (-1)^r a_r \tag{19}$$

Proof. We know that $10 \equiv -1 \bmod 11$.

$$\begin{aligned} n &= 10^r a_r + 10^{r-1} a_{r-1} + \ldots + 10^1 a_1 + a_0 \\ &\equiv (-1)^r a_r + (-1)^{r-1} a_{r-1} + \ldots + (-1)^1 + a_0 \end{aligned} \tag{20}$$

Which is the definition of this divides rule (where the plus and minus alternatives for every term). □

$$2 - 8 + 5 - 9 + 1 - 0 + 3 = -6 \tag{21}$$

So no, 11 does not divide 3019582.

6)

Proof.

$$n = 10^r a_r + 10^{r-1} a_{r-1} + \ldots + 10^1 a_1 + a_0 \tag{22}$$

The division rule for 7 can be written as follows:

$$3 \sum_{i=1}^{r} 10^{i-1} a_i + a_0 \equiv 0 \bmod 7 \tag{23}$$

We know that $3 \equiv 10 \bmod 7$, so we can sub that in and bring the coefficient into the sum.

$$\begin{aligned} \left(\sum_{i=1}^{r} 10^i a_i \right) + a_0 &\equiv 0 \bmod 7 \\ \underbrace{\sum_{i=0}^{r} 10^i a_i}_{n} &\equiv 0 \bmod 7 \end{aligned} \tag{24}$$

So therefore $n \equiv 0 \bmod 7$ when this rule holds. □

7)

7.a)

$$\begin{aligned} 1 &\mapsto 9 \\ 0 &\mapsto 4 \\ 13 &\mapsto 17 \end{aligned} \tag{25}$$

🍌

$$(9)(4)(17)(4)(17)(4) \tag{26}$$

Decrypting these using the following Python code yields ("JERERE")

```
chr(x + 97)
```

Where `x` is the numeric character code (0 is A…).

7.b)

We can find the inverse of 5 in mod 26.

$$5 \cdot 21 \equiv 1 \bmod 26 \tag{27}$$

So 21 is the inverse of 5 in mod 26.

$$\begin{matrix} M & E & R & I & W \\ 12 & 4 & 17 & 8 & 22 \end{matrix} \tag{28}$$

M

$$\begin{aligned} 5x + 4 &\equiv 12 \bmod 26 \\ 5x &\equiv 8 \bmod 26 \\ 21(5x) &\equiv 168 \bmod 26 \\ x &\equiv 12 \bmod 26 \end{aligned} \tag{29}$$

So $M \mapsto M$

E

$$\begin{aligned} 5x + 4 &\equiv 4 \bmod 26 \\ 5x &\equiv 0 \bmod 26 \\ x &\equiv 0 \bmod 26 \end{aligned} \tag{30}$$

So $A \mapsto E$

R

$$\begin{aligned} 5x + 4 &\equiv 17 \bmod 26 \\ 5x &\equiv 13 \bmod 26 \\ 21 \cdot 5 &\equiv 13 \cdot 21 \bmod 26 \\ x &\equiv 13 \bmod 26 \end{aligned} \tag{31}$$

So $N \mapsto R$

I

$$\begin{aligned} 5x + 4 &\equiv 8 \bmod 26 \\ 5x &\equiv 4 \bmod 26 \\ 21 \cdot 5x &\equiv 84 \bmod 26 \\ x &\equiv 6 \bmod 26 \end{aligned} \tag{32}$$

So $G \mapsto I$

W

$$
\begin{aligned}
5x + 4 &\equiv 22 \bmod 26 \\
5x &\equiv 18 \bmod 26 \\
12 \cdot 5 &\equiv 18 \cdot 21 \bmod 26 \\
x &\equiv 14 \bmod 26
\end{aligned} \tag{33}
$$

So $O \mapsto W$.

MANGO 🥭

8)

8.a)

$ax \equiv k \bmod m$ has a solution if and only if $(a, m) \mid k$.

Proof. $(\Longrightarrow)$

$$ax = k + ml \tag{34}$$

for some $l \in \mathbb{Z}$

Let $a = \alpha(a, m)$ and $m = u(a, m)$.

Then:

$$
\begin{aligned}
ax - ml &= k \\
\Longrightarrow \quad (a, m)\underbrace{(\alpha x - ul)}_{\in \mathbb{Z}} &= k
\end{aligned} \tag{35}
$$

So $(a, m) \mid k$.

$(\Longleftarrow)$

(1) we know that $(a, m)l = k$.
(2) we know that $(a, m) = ax + my$ (Bezout's identity)

Then subbing (2) into (1).

$$
\begin{aligned}
(az + my)l &= k \\
azl + myl &= k \\
a\underbrace{(zl)}_{x} = k + m&\underbrace{(-yl)}_{\in \mathbb{Z}}
\end{aligned} \tag{36}
$$

So $ax \equiv k \bmod m$. $\square$

8.b)

Choose $a = 5, m = 10, k = 5$. Then $(a, m) = 5$.

$$5x \equiv 5 \bmod 10 \tag{37}$$

Solutions to x are $1, 3, 5, 7, 9$, which is $5 = (a, m)$ solutions...

Choose $a = 2, m = 8, k = 2$. Then $(a, m) = 2$.

$$2x \equiv 4 \bmod 8 \tag{38}$$

Solutions to x are $2, 6$, which is $5 = (a, m)$ solutions...

So my conjecture is: *If $(a, m) \mid k$, then the equation $ax \equiv k \bmod m$ has exactly (a, m) solutions modulo m.*

9)

9.a)

Proof. Let $z = a_1 + b_1$ and $w = a_2 + b_2$.

Then:

$$\begin{aligned} z \cdot w &= (a_1 + b_1 i)(a_2 + b_2 i) \\ &= (a_1 a_2 - b_1 b_2) + i(a_1 b_2 + a_2 b_1) \end{aligned} \tag{39}$$

The norm of $z \cdot w$ is:

$$\begin{aligned} N(zw) &= (a_1 a_2 - -b_1 b_2)^2 + (a_1 b_2 + a_2 b + 1)^2 \\ &= a_1^2 a_2^2 + b_1^2 b_2^2 - 2a_1 a_2 b_1 b_2 + a_1^2 b_2^2 + a_2^2 b_1^2 + 2a_1 a_2 b_1 b_2 \\ &= a_1^2 a_2^2 + b_1^2 b_2^2 + a_1^2 b_2^2 + a_2^2 b_1^2 \\ &= (a_1^2 + a_2^2)(b_1^2 + b_2^2) \\ &= N(z)N(w) \end{aligned} \tag{40}$$

Therefore, $N(zw) = N(z)N(w)$. □

9.b)

Proof. Suppose there exists $x, y \in \mathbb{Z}[i]$ such that $x \cdot y = 2 + i$.

Then:

$$\begin{aligned} N(x)N(y) &= N(2 + i) \\ &= 5 \end{aligned} \tag{41}$$

So $N(x)$ (or $N(y)$) can only be 1 or 5 as 5 is prime in $\mathbb{Z}$. But because the norm of $2 + i$ can only be factored into two terms, we conclude that $2 + i$ is prime in $\mathbb{Z}[i]$. We can complete the same steps for $2 - i$ because it has the same norm as $2 + i$ to show that $2 - i$ is prime in $\mathbb{Z}[i]$.

Because $2 + i \mid 5$ but $N(2 + i) = 5 \neq 1$ or $N(5)$, we conclude that 5 is not prime in $\mathbb{Z}[i]$. □

9.c)

Proof. $p \in \mathbb{Z}$ is prime.

Choose $x \cdot y = p$. Then:

$$\begin{aligned} N(x)N(y) &= N(p) \\ N(x)N(y) &= p^2 \end{aligned} \tag{42}$$

So $N(x) = 1, p,$ or p^2 since p is prime. We choose $N(x)$ instead of $N(y)$ (without loss of generality), but the same cases apply to $N(y)$.

If $N(x) = 1, p^2$ then we have satisfied the requirements p being prime in $\mathbb{Z}[i]$.

If $N(x) = p$ and $x = a + bi$, then $N(x) = a^2 + b^2$. Since $p = a^2 + b^2 \equiv 3 \bmod 4$, we know that such an a and b cannot exist to give congruence mod 4, so $N(x)$ is never equal to p.

So... $N(x) = 1$ or $N(x) = p^2 = N(p)$. So p is prime in $\mathbb{Z}[i]$ $\square$

9.d)

$$13 = (2 + 3i)(2 - 3i) \tag{43}$$

If $xy = 2 + 3i$, then $N(x) = 1$ or 13, so $2 \pm 3i$ is prime in $\mathbb{Z}[i]$.